

HOW IT WORKS

Windows Vista

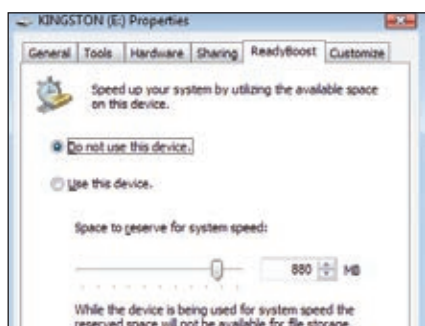
You may have been desperate to get your hands on a copy of Microsoft's new operating system, but how much do you know about the technologies that make those dazzling features possible? Tom Royal sheds some light on Windows Vista

If you've recently upgraded to Windows Vista, or bought a new computer with it preinstalled, you've probably noticed the flashy new interface, upgraded file browsers and redesigned Start menu. Look a little closer, though, and you'll find some clever new technologies tucked away inside. This month, we explain the mechanics behind some of the most interesting new tools and technologies in Microsoft's latest operating system.

TRACE MEMORY

Microsoft recommended a minimum of 128MB of memory for Windows XP, and that was wildly optimistic (512MB or ideally 1GB is a sensible amount). For most editions of Windows Vista, Microsoft recommends having at least 1GB of memory. With more memory needed just to run the operating system, Microsoft has implemented two clever technologies to make the most of the memory in your PC. SuperFetch and ReadyBoost are included in all versions of Vista, including the Home Premium edition.

SuperFetch is an extension to a technology that's been around for some time. Virtual memory was first introduced to Microsoft's operating systems in Windows 3. It allows you to use a chunk of your hard disk, often referred to as a page file, as extra memory. Transferring data to and from a hard disk is far slower than moving it in and out of memory, though, so virtual memory needs to be used judiciously. Say your computer needs to store 1GB of data in memory, but you have only 512MB of physical memory. 512MB of your data must be stored in virtual memory. Windows manages that virtual memory on demand; only when a running program needs to access paged data does Windows move it back to main memory. Behind the scenes, when you switch to an application that requires some of the data stored in virtual memory, an error, known as a page fault, is generated. Windows moves the needed data back into physical memory to be accessed.



▲ ReadyBoost allows you to use a portion of a USB thumb drive as extra virtual memory

You can see how much virtual memory data is in use on your hard disk by viewing the Performance tab of the Windows Task Manager. The graph labelled PF Usage shows the size of the virtual memory in megabytes. If you open lots of memory-hungry applications at once and switch between them, your computer lags. If you use a computer with very little memory to run a memory-hungry application, the constant need to transfer information to and from the hard disk can have a severe impact on performance.

Windows XP introduced a new virtual memory technology called Prefetch. This analyses the data used by applications, and moves it all into physical memory when a program is activated to minimise the number of page faults. Windows XP monitors the page faults created during key periods of operation, such as the boot process and the first 10 seconds from an application being launched. It records the data that is fetched during this period, and logs it to a file in the C:\Windows\Prefetch directory. This directory has many files with the extension .pf. Most have a name that begins with the application to which they relate, followed by eight hexadecimal characters, such as NOTEPAD.EXE-2F2D61E1.pf.

When you start a program, Windows XP checks the Prefetch directory to see if it contains a file with information about the application. If it does, it halts the application and loads all the relevant data into physical memory before continuing in an effort to speed up the program's launch. The same process takes place during system startup. Information on page faults during startup is stored in a special file in the \Windows\Prefetch directory whose name begins with NTOSBOOT. Windows also performs a periodic analysis of the data stored in the Prefetch folder. It then rearranges data on your hard disk so bytes of data that are fetched together during system or application startup are placed physically next to one another on the hard disk, allowing them to be read faster.

Although it helps to accelerate the launch of applications, the Prefetch system in Windows XP is still demand-based, and takes action only once an application has been launched. Windows Vista's new prepaging system, SuperFetch, goes one step further. As well as monitoring the data needed when an application is launched, it also tracks the time and day of the week on which applications are started and used. You can spot SuperFetch working by examining the Performance tab of the Windows Vista Task Manager. Even if you have only a few windows open, you'll notice that a surprising amount of your available physical memory is used up; this is the result of SuperFetch stuffing unused memory

full of data that might be required by other applications you often use.

FLASH IN THE PAN

SuperFetch runs as a service on Windows Vista from the moment you start your computer, so you don't need to do anything to get it working. If your computer is still not performing as well as you'd like, though, there is another Windows Vista feature you can enable to try speeding it up. ReadyBoost allows you to use a USB flash drive as extra memory for your computer.

ReadyBoost uses a special page file, created on a USB flash drive, as virtual memory. This is beneficial because, although flash memory is nowhere near as fast as the DDR or DDR2 memory inside your computer, it is quicker than a hard disk when moving small and non-sequential chunks of data. One blog posting on Microsoft's MSDN website estimates that reading a random 4KB page of data from flash memory is roughly 10 times faster than doing so from the hard disk. Using a flash drive for something as vital as memory management has one obvious problem: the user can remove it from the PC at any time. This has the potential to create havoc for the operating system, and could also present a security problem if the data stored on the flash drive can be examined. To avoid these problems, all the data stored on the flash drive is encrypted using a 128-bit AES algorithm, and backed up on the hard disk.

Although it gives an effect that's similar to adding more memory, ReadyBoost is not a substitute for fitting more memory to your computer. Instead, ReadyBoost is designed for those who cannot add more system memory. Matt Ayers, program manager at Microsoft's Windows Client Performance group, has written that "the feature is designed to improve small random I/O for people who lack the expansion slots, money and/or technical expertise to add additional RAM... Adding RAM is still the best way to relieve memory pressure."

ReadyBoost is easy to set up. When you plug in a suitable flash drive, ReadyBoost shows up as an option on the pop-up menu that appears. It requires a USB2 flash memory device with a capacity of at least 256MB. Not all flash drives are suitable; Windows tests the drive to ensure it can perform 4K random data reads at 2.5MB/s, and 512K random data writes at 1.75MB/s. You can't use a ReadyBoost cache file of larger than 4GB, as this is the largest single file size allowed by the FAT32 file system.

THROW AWAY THE KEY

As well as giving your computer a speed boost, Windows Vista includes new features that can

help you make it more secure. One of the most interesting is BitLocker drive encryption, which is included in the Ultimate and Enterprise editions. BitLocker allows you to secure the data on your computer by encrypting the hard disk partition that contains Windows. It's designed to work best for businesses using a group security policy and computers equipped with a special security chip, but Windows Vista Ultimate users can secure their PC using a standard USB flash drive.

BitLocker is based on AES encryption. Unlike public key cryptography, which we explained in *How it Works*, *Shopper* July 2006, AES is a symmetric key method. It uses a single key to encrypt and decrypt rather than a public key to encrypt and a private key to decrypt. This said, AES is far more secure than simpler symmetric encryption methods such as DES. In 2003, 128-bit AES encryption was validated by the US government as secure enough for use with secret classified information, and 256-bit AES as secure enough for use with top-secret information. BitLocker can use 128-bit or 256-bit AES.

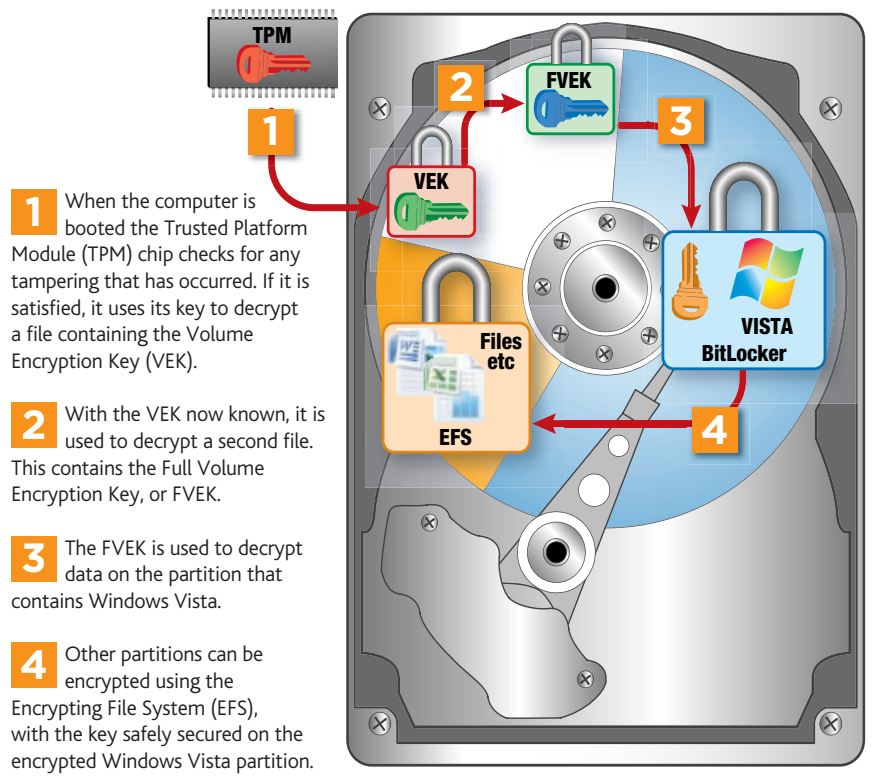
To use BitLocker, you first need to set up your PC's hard disk. As well as the main disk partition, which contains all the Windows Vista files and is fully encrypted during use, you need a second partition. This must be at least 1.5GB in size, and unencrypted. The computer's BIOS is set to boot from this second, unencrypted, volume. BitLocker can encrypt only one partition itself, but other partitions you might have can be secured using the Encrypting File System (EFS). The keys for this encryption are then stored on the Windows partition, which is itself encrypted, so they are locked by the same system.

BitLocker can be set up in one of four ways. The first three require a special chip known as a Trusted Platform Module (TPM) on the computer's motherboard. The TPM can perform cryptographic functions and contains a pair of encryption keys that are unique to that chip. This enables BitLocker to detect if the system hard disk is removed from one computer (with one TPM) and placed in another (with a different or no TPM) for analysis. The TPM forms the basis of the simplest BitLocker system. When the PC is booted, it follows a complicated sequence of loading and decrypting to produce the key used to decrypt the hard disk. We explain it step by step:

1. A file is loaded from the hard disk. This contains the Volume Encryption Key (VEK), which has been encrypted using data inside the TPM chip.
2. The TPM checks the boot files on the unencrypted partition to see if the computer has been tampered with. If it is satisfied that nothing untoward has taken place, it decrypts the VEK file to produce the VEK.
3. A second file is loaded from the hard disk. This contains the Full Volume Encryption Key (FVEK), which has been encrypted using the VEK.
4. As the VEK is already known, the computer can decrypt the FVEK file to access this second key. Once the FVEK is known, the system can access the contents of the FVEK-encrypted hard disk partition that contains Windows.

At first glance, this process looks overly complicated, and the VEK seems redundant.

Key issues BitLocker drive encryption



After all, it would be possible to have the TPM simply decrypt the FVEK itself, cutting out two steps. The reason for the VEK is one of convenience. Without it, changing the encryption on the computer would require a change of FVEK, which would require the entire Windows partition to be re-encrypted. With this system, the VEK can be changed instead, and the only file that would need re-encrypting is the small one holding the FVEK.

This system is designed to run without the user's intervention, or even without the user's knowledge. If more security is required, though, extra authentication can be added in Step 2. The user may be required to enter a PIN on the keyboard, or plug in a USB flash drive containing an extra key. The system will wait for this extra authentication before continuing to decrypt the other keys and load the system.

CENSOR SENSITIVITY

Trusted Computing technology, of which the TPM chip is a key part, is particularly controversial. Ross Anderson, who leads the computer security group at Cambridge University, has suggested a particularly dystopian future should Trusted Computing catch on:

"The potential for abuse extends... into political censorship. I expect that it will proceed a step at a time. First, some well-intentioned police force will get an order against a pornographic picture of a child, or a manual on how to sabotage railroad signals. All TC-compliant PCs will delete, or perhaps report, these bad documents. Then a litigant in a libel or copyright case will get a civil court order against an offending document... A dictator's secret police could punish the author of a dissident leaflet by deleting everything she ever created using that system... Once lawyers, policemen and judges realise the potential, the trickle will become a flood."

For the moment TPM chips are rare, and *Computer Shopper* hasn't yet reviewed a computer fitted with one. If you want to secure your computer with BitLocker, though, there is an easier and less controversial way to do so. Instead of using a TPM to encrypt the keys required to start your PC, you can use a key stored on a USB flash drive. This flash drive must then be inserted into the computer each time you start it as without the drive, you'll find that Windows will not boot.

There's always a danger that you might lose the flash drive with this key. Alternatively, your motherboard might fail, giving you good reason to want to install the hard disk in another computer. BitLocker provides a method for you to do so. When BitLocker is enabled, a separate key, known as the recovery key, is generated. In a company network, this file will be stored on a secure server elsewhere in the building, but home users can place it on another USB drive, or even print it out. If all else fails, you can tell BitLocker to enter recovery mode. As long as BitLocker can read this key from a flash drive, or you can type it in, you can access your disk. **ES**

FURTHER INFORMATION

Matt Ayers' Q&A on ReadyBoost
<http://blogs.msdn.com/tomarcher/archive/2006/06/02/615199.aspx>

White paper on Vista performance acceleration
www.microsoft.com/whdc/system/sysperf/perfaccel.mspx

BitLocker technical overview (Microsoft)
<http://technet.microsoft.com/en-us/windowsvista/aa906017.aspx>

Ross Anderson on Trusted Computing
www.cl.cam.ac.uk/~rja14/tcpa-faq.html